IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

SAMUEL DONETS, individually and on behalf of all others similarly situated, Plaintiff, vs. **VIVID SEATS LLC,** a Delaware limited liability company, Defendant.	Case No.: 1-20-cv-03551 Honorable Franklin U. Valderrama **JURY TRIAL DEMANDED**

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Samuel Donets ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class"), through counsel, for his first amended complaint against defendant, Vivid Seats LLC, states:

NATURE OF THE CASE

1. This is a class action arising out of the defendant's unlawful collection, use, retention and disclosure of the personal biometric identifiers and biometric information of Plaintiff and the Class in violation of the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 (2008).

THE PARTIES

2. Plaintiff, Samuel Donets ("Plaintiff"), is a natural person who resides in Glenview, Illinois.

3. Defendant, Vivid Seats LLC ("Vivid"), is a limited liability company formed and existing under the laws of the state of Delaware.

4. Vivid is registered with the Illinois Secretary of State to do business in Illinois and maintains one or more offices in Illinois.

5. Vivid operates a ticket and event marketplace where tickets to concerts, shows and sporting events are marketed and sold to consumers throughout the world. According to Vivid's Facebook profile, it "is the leading independent online ticket marketplace, sending tens of millions of fans to live events every year."[1]

6. Vivid operates the web site www.vividseats.com.

7. Vivid maintains its principal offices and operates one or more call centers in Illinois where it employs individuals to, *inter alia*, respond to telephone and internet inquiries and to process marketplace orders.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). The amount in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and is a class action in which there are numerous class members who are citizens of states different from Defendant. The number of members of the proposed class is in the aggregate greater than 100 and more than two-thirds of the class members reside in states other than the state in which Defendant is a citizen.

9. This Court has personal jurisdiction over Defendant because its principal place of business is in Illinois, it conducts substantial business in Illinois, and a substantial portion of the acts complained of took place in Illinois.

[1] facebook.com/VividSeats/ last visited on June 15, 2020 at 6:49 p.m.

10. Venue lies in this District pursuant to 28 U.S.C. §1391(b) and 1400(a) as a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District and Vivid resides and may be found in this District.

SUMMARY OF CLAIMS

11. Employees of Vivid, including Plaintiff and members of the Class, are required as a condition of employment to have their fingerprints scanned and stored in a system Vivid maintains for time tracking and employee authentication.

12. While there are tremendous benefits to using biometric time clocks in the workplace, there are also serious risks. Unlike key fobs or identification cards—which can be changed or replaced if stolen or compromised—fingerprints are unique, permanent biometric identifiers associated with the employee. This exposes employees to serious and irreversible privacy risks. For example, if a fingerprint database is hacked, breached, or otherwise exposed, employees have no means by which to prevent identity theft and unauthorized tracking. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, and Facebook/Cambridge Analytica data breaches or misuses – employees have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

13. A nefarious market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion

Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018).[2]

14. In late 2007, a biometrics company called Pay by Touch - which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions - filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records - which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data - could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who had used that company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

15. Recognizing the need to protect its citizens from situations like these, in 2008, Illinois enacted BIPA in light of the "very serious need [for] protections for the citizens of Illinois when it comes to [their] biometric information."[3]

16. Biometrics are unlike other unique identifiers used to access finances or other sensitive information. "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the

[2] Available at https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259f138.

[3] 95th Ill. Gen. Assem. House Proceedings, May 30, 2008, at 249 (statement of Representative Ryg), available at http://www.ilga.gov/house/transcripts/htrans95/09500276.pdf.

individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[4]

17. To address this legitimate concern, Section 15(b) of BIPA provides that:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.[5]

18. For BIPA purposes, a "biometric identifier" is a personal feature that is unique to an individual and specifically includes fingerprints.

19. BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based upon an individual's biometric identifier used to identify the individual.[6]

20. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it *first*:

---

[4] 740 ILCS 14/5(c).
[5] 740 ILCS 14/15(b).
[6] *Id.*

> (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information.

740 ILCS 14/15(b).

21. BIPA specifically applies to employees who work in the State of Illinois.

22. BIPA defines a "written release" specifically "in the context of employment [as] a release executed by an employee as a condition of employment." 740 ILCS 14/10.

23. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and—most importantly here—fingerprints. *See* 740 ILCS 14/10. Biometric information is separately defined to include any information based on an identifier that is used to identify an individual. *See id.*

24. BIPA also establishes standards for how employers must handle Illinois employees' biometric identifiers and biometric information. *See* 740 ILCS 14/15(c)-(d). BIPA makes it unlawful for companies to "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." Furthermore, no company may "disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless":

> (1) the person or customer consents to the disclosure or redisclosure;
>
> (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the person or customer;
>
> (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

See 740 ILCS 14/15(c)-(d).

25. Ultimately, the BIPA is simply an informed consent statute. Its narrowly tailored provisions place no absolute bar on the collection, sending, transmitting or communicating of biometric data. For example, the BIPA does not limit what kinds of biometric data may be collected, sent, transmitted, or stored. Nor does the BIPA limit to whom biometric data may be collected, sent, transmitted, or stored. The BIPA simply mandates that entities wishing to engage in that conduct must make proper disclosures and implement certain reasonable safeguards.

FACTS RELATED TO PLAINTIFF

26. Plaintiff worked for Vivid in Illinois in 2014-2015 at Vivid's Illinois call center.

27. Since at least 2015, Vivid required employees to scan their fingerprints at the start and conclusion of each day and each time they left and returned from lunch or break.

28. Vivid employs hundreds of persons in Illinois and over the course of the last five years it has employed at least 500 persons in Illinois.

29. Each time a Vivid employee began and ended a workday, and when he left and returned from lunch or break, Vivid required a scan of the employee's fingerprints. Plaintiff's fingerprints were scanned no less than four times each day that he worked for Vivid and hundreds of times over the course of his employment by Vivid.

30. Vivid never informed Plaintiff of the specific limited purposes or length of time for which it collected, stored, or used fingerprints.

31. Similarly, Vivid never informed Plaintiff of any biometric data retention policy it developed, nor whether it will ever permanently delete fingerprints.

32. Plaintiff never signed a written release allowing Vivid to collect or store fingerprints.

33. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Vivid's violations of the BIPA alleged herein.

34. Plaintiff now seeks damages under BIPA as compensation for the injuries Vivid has caused.

CLASS ALLEGATIONS

35. Plaintiff brings this action under Rule 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure on behalf of the following class of persons aggrieved by Vivid's BIPA violations subject to modification after discovery and case development:

> All residents of Illinois who are current and former employees of Vivid who had any biometric identifier or biometric information collected, captured or received by Vivid without disclosures and consent during the five (5) year period preceding the filing of this action.

36. Class members are identifiable through Vivid's records and payment databases.

37. Excluded from the Class are: (1) any Judge presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

38. Vivid's actions have harmed Plaintiff and the Class members.

39. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but it is clear that individual joinder is impracticable. Defendant has collected, captured,

received, or otherwise obtained biometric identifiers or biometric information from more than 500 employees who fall into the definition of the Class. Ultimately, the Class members will be easily identified through Defendant's records.

40. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

(a) Whether Vivid collected Biometric Identifiers from Plaintiff and the Class in the form of their fingerprints.

(b) Whether Vivid failed to inform Plaintiff and the Class in writing that their biometric identifier(s) were being collected.

(c) Whether Vivid failed to inform Plaintiff or the Class in writing of the specific purpose and length of term for which the fingerprints were being collected, stored and used.

(d) Whether Vivid failed to obtain Plaintiff and the Class's informed consent for the use of their fingerprints.

(e) Whether Vivid did not obtain a written release from Plaintiff or the Class authorizing the use of their fingerprints.

(f) Whether Vivid failed to provide any other alternative method for Plaintiff or the Class to clock in and out of work which effectively denied Plaintiff and the Class any meaningful alternative to avoid use of their fingerprints.

41. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial

resources to do so. Neither Plaintiff nor their counsel have any interest adverse to those of the other members of the Class. Plaintiff's claims are typical of the claims of the Class.

42. **Appropriateness**: This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in their Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

COUNT ONE

Violation of §15(b) of BIPA
[Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information]

43. Plaintiff realleges all prior paragraphs of the complaint as if set out here in full.

44. BIPA requires companies to obtain informed written consent from employees before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in

writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS 14/15(b) (emphasis added).

45. Defendant fails to comply with these BIPA mandates.

46. Defendant is an entity registered to do business in Illinois and thus qualifies as a "private entity" Under BIPA. *See* 740 ILCS 14/10.

47. Plaintiff and the Class are each individuals who had "biometric identifiers" (in the form of fingerprints) collected by Defendant. *See* 740 ILCS 14/10.

48. The biometric identifiers Plaintiff and the Class were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

49. Defendant systematically and automatically collected, used, stored, and disclosed biometric identifiers and/or biometric information of Plaintiff and the Class without first obtaining the written release required by 740 ILCS 14/15(b)(3).

50. Defendant did not inform Plaintiff and the Class in writing of the specific length of term for which biometric identifiers and/or biometric information were being collected, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

51. By collecting, storing, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, each Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA *each time* the Defendant collected, stored or used Plaintiff's or the Class's biometric identifier. *See* 740 ILCS 14/1, *et seq*.

52. Plaintiff and the Class seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT TWO

Violation of §15(d) of BIPA
[Disclosure of Biometric Identifiers and Information Before Obtaining Consent]

53. Plaintiff realleges all prior paragraphs of the complaint as if set out here in full.

54. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

55. Defendant fails to comply with this BIPA mandate.

56. Defendant is an entity registered to do business in Illinois and thus qualifies as a "private entity" Under BIPA. *See* 740 ILCS 14/10.

57. Plaintiff and the Class are each an individual who had their "biometric identifiers" (in the form of their fingerprints) collected by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

58. The biometric identifiers of Plaintiff and the Class were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

59. Upon information and belief, by utilizing a biometric time clock, Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated biometric

identifiers and/or biometric information of Plaintiff and the Class to at least the payroll company hired by the Defendant without first obtaining the consent required by 740 ILCS 14/15(d)(1).

60. By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class's biometric identifiers and biometric information as described herein, each Defendant violated BIPA *each time* there was a disclosure, redisclosure or dissemination of the Plaintiff's or Class's biometric identifiers in violation of Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

61. Plaintiff and the Class seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff individually and for the Class, respectfully request that the Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing Plaintiff's counsel as Class Counsel;

B. Declaring that Defendant's actions, as set out above, violate the BIPA;

C. Awarding damages for each of Defendant's violations of the BIPA, pursuant to 740 ILCS 14/20;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including an Order requiring Defendant to collect, store, and use biometric identifiers or biometric information in compliance with the BIPA;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees; and

F. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees.

JURY DEMAND

Plaintiff, Samuel Donets, on behalf of himself and all others similarly situated, hereby respectfully demands a trial by jury on all such claims that may be so tried.

Dated: October 16, 2020

Respectfully submitted,

SAMUEL DONETS,
individually and on behalf of all others similarly situated,

/s/ Nick Wooten
Nick Wooten - *Lead Trial Counsel*
Nick Wooten, LLC
5125 Burnt Pine Drive
Conway, Arkansas 72034
(833) 937-6389
nick@nickwooten.com

Rusty A. Payton
Payton Legal Group
20 North Clark Street
Suite 3300
Chicago, Illinois 60602
(773) 682-5210
info@payton.legal

Arthur C. Czaja
7521 N. Milwaukee Ave.
Niles, Illinois 60714
(847) 647-2106
arthur@czajalawoffices.com

Counsel for Plaintiff and the Class

CERTIFICATE OF SERVICE

The undersigned certifies that on October 16, 2020, a true and correct copy of the foregoing First Amended Class Action Complaint was served upon counsel of record via electronic filing.

/s/ Nick Wooten
Nick Wooten

Counsel for Plaintiff and the Class